



Understanding IT Governance and Risk Management.



Minimizing Risk

& Maximizing Opportunity



**"Jack stands?
Hah! Who needs
'em?"**





**Necessity is the
mother of
invention...**





“And to think... those wimps at the power company use straps and cleats to get up this high!”





**I'm sure this guy still
wonders why he got
fired over this!**





Step 1: Remove shoes

**Step 2: Place metal
ladder in water**

**Step 3: Begin using
power tools while
standing barefoot on
metal ladder in water**





And the winner is...

**How drunk do you have to be
before this starts looking like
a good idea?**





“Gee, guys... that seems like an awful lot of protective gear for such a small chlorine gas leak...” (I’m guessing the guy in the pink shirt is a politician)



DTs Session Overview

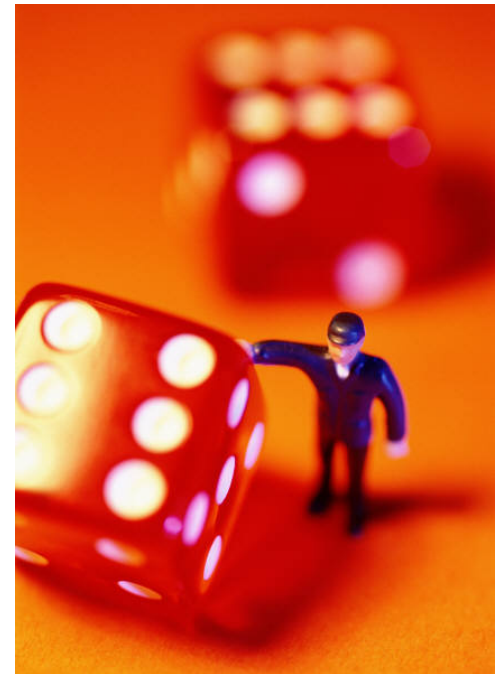
- *What is Risk*
- *How do I analyze (measure) it*
- *How do I know what to do with it*
 - What are my choices*
- *How do I communicate it*
- *What does it mean to management*

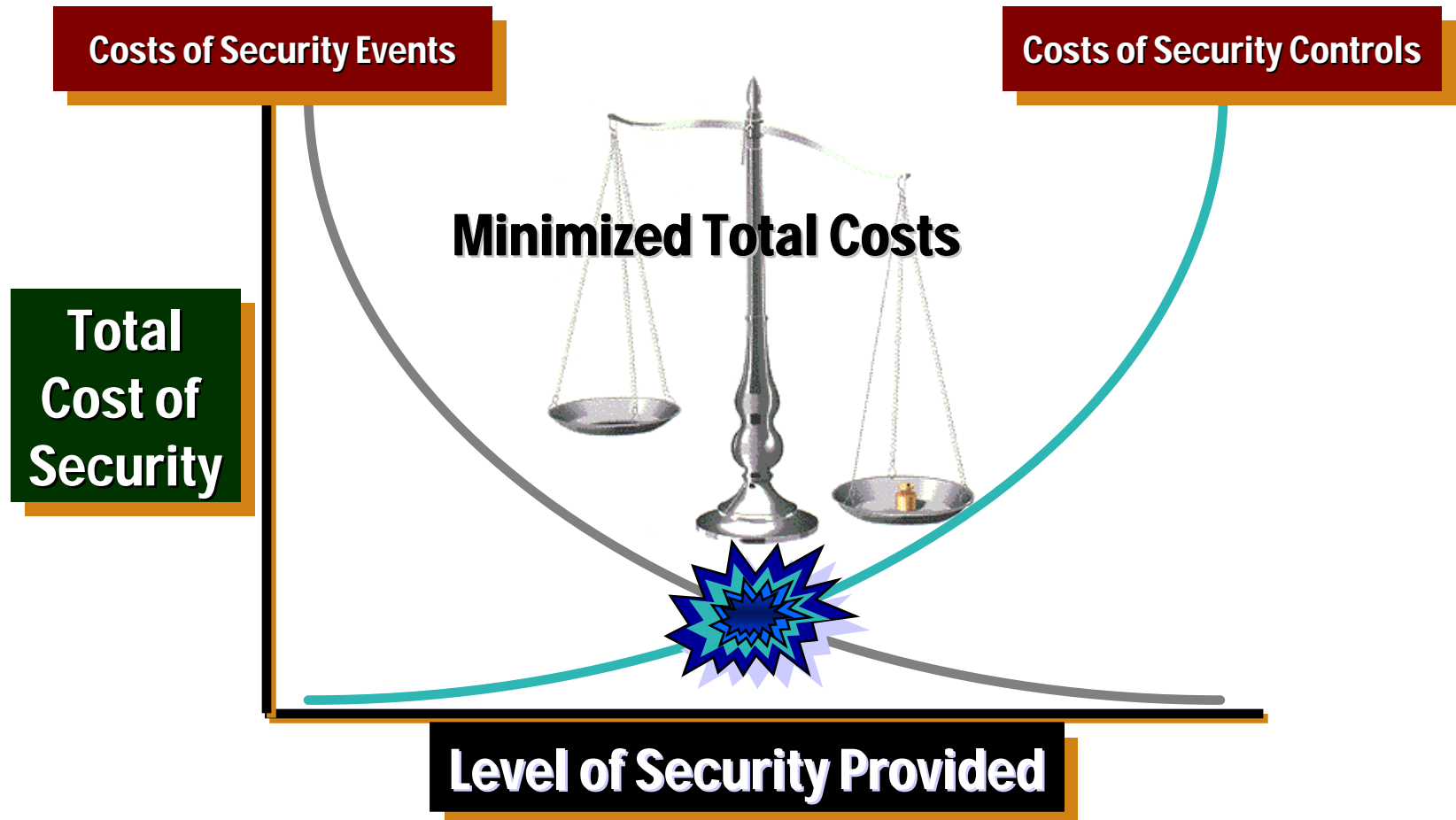




What is security risk analysis?

Can be defined as the practice of ensuring that controls and expenditure are fully commensurate with the risks to which the organization is exposed.







Identifying exposures and managing associated risks increases your appeal to customers, stakeholders, business partners, and regulators.

A stable and prepared business builds trust with its:

- Customers
- Regulators
- Stakeholders
- Business partners

Increased customer satisfaction and retention:

- Lower total operating expenses
- Optimized expenditures
- Enhanced public value





Three KEY elements of a successful risk reduction program:

- Knowledge of Threat
- Knowledge of Vulnerability
- Knowledge of Business Value/Event Cost

$$\text{Risk} = \text{Threat} * \text{Vulnerability} * \text{Event Cost}$$



- Threat:

The likelihood that a security event will happen in a given time span or the rate.

Security Event Rate (per month, hour etc.)

Composed of world-wide rate modified by local Target Index, & other factors.

The threat of purse-snatching by breaking the passenger window of a car with a heavy object was zero nationwide in 1960 (it never happened)

The threat became significant in Miami in 1970

The threat in Iowa City is still zero.



- Vulnerability:

A given target is either vulnerable or not to a particular well defined threat (0 or 1).

A given target is variably vulnerable to a class of threats. (Vulnerability between 0 and 1)

A given organization is composed of numerous targets which, as a group, are variably vulnerable to a given threat category (*Vulnerability Index*)

Car passenger windows have always been vulnerable to breakage by heavy bricks moving fast enough

Since there was no threat until 1970,
there was no risk until 1970.



- EventCost:

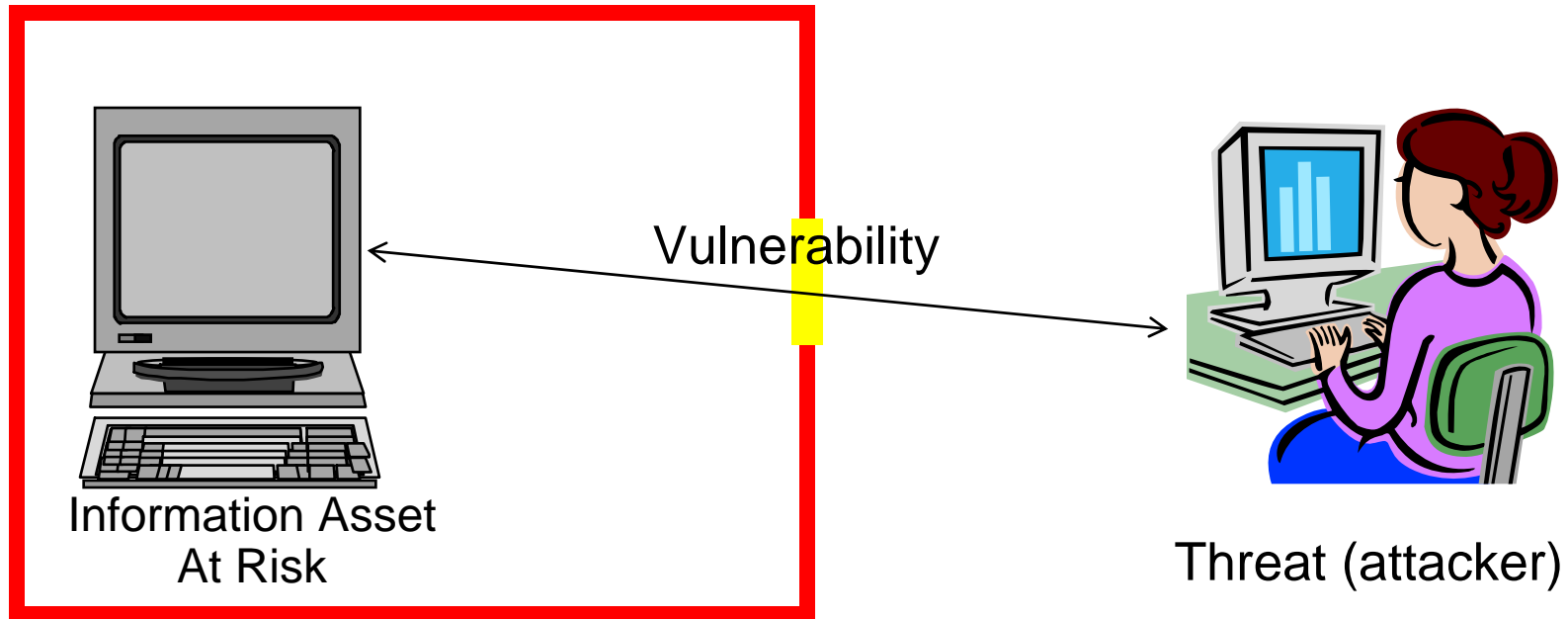
Security Events result from a threat successfully exercised against a vulnerable system.

The total costs of all of the ramifications of a security event are made up of numerous factors and include both hard and soft costs.

Total sum of all ramifications of a security event called
EventCost *Dollars per SecurityEvent*



Risk Concept



Risk analysis starts with understanding what assets are potentially at risk, what the threats are, and what are the vulnerabilities that could be exploited. This forms the basis for finding the “**sweet spot**” of putting in enough security for to protect the value of the assets.



The Sea Of Risk

Internal:

- Hacking tools and discovery tools
- Unauthorized applications
- Unauthorized communications
- Counterfeiting/ fraud
- Rogue servers and services
- Wrongful Termination
- Fraud
- Mishandling and theft of IP
- Theft of customer information
- Harassment
- Possession of Inappropriate material
- Computer file deletion/destruction

External:

- Unauthorized users/ intruders
- Vandalism
- DoS attacks
- IP piracy





© Cartoonbank.com



*"We're too well connected for jail time, but I worry
a little about middle management."*



How can it benefit my organization?

- Cost justification - ROI?
 - Enhance productivity - Not Likely
 - Break barriers - Creates them
 - Security awareness - OK, I'll give you that
-
- Reduce Executive Liability
Negligence
 - Fines
 - SOX – Up to \$5million and imprisonment.
 - GLBA – Up to \$500k and imprisonment
 - HIPAA – Up to \$250k and imprisonment
 - SEC - \$MM fines
 - Embarrassment
 - Policy Violations





Get Management Involved

- Information Risk Management Committee
 - Two individuals from each Division
 - Must be members of the Division Information
- **Division Information Risk Assessment Group**
 - One or Two members from each Office/Department Risk Assessment Team
- **Office/Department Risk Assessment Team**
- Identify a few interested Offices/Departments in each division
- Set up Office/Departments Risk Assessment Teams
- Provide training in Risk Assessment
 - Office/Department Risk Assessment Teams
 - Division Information Risk Assessment Group
- Tailor Risk Assessment tools to meet the needs of each Department/Office



Alphabet Soup

ISO 17799

OCTAVE

CobiT

ITIL

NIST 800

COSO

HIPAA



What Good Is Alphabet Soup?

- Choices
- Nice thing about these choices
 - No bad choices
 - Just bad implementations
- Pick a Comprehensive Framework
- Pick a Risk Assessment Methodology
- Pick a Verification Program
- ... and stick with them



Why NIST

- NIST provides consistent, comparable, and neutral perspective
- As a result of the review process, NIST obtains better understanding of Federal agency/program needs for guidance

State of California relies on Federal Guidelines (OMB –A130, etc)

- NIST efforts help meet statutory responsibilities

Provide technical assistance in implementing standards and guidelines, including:

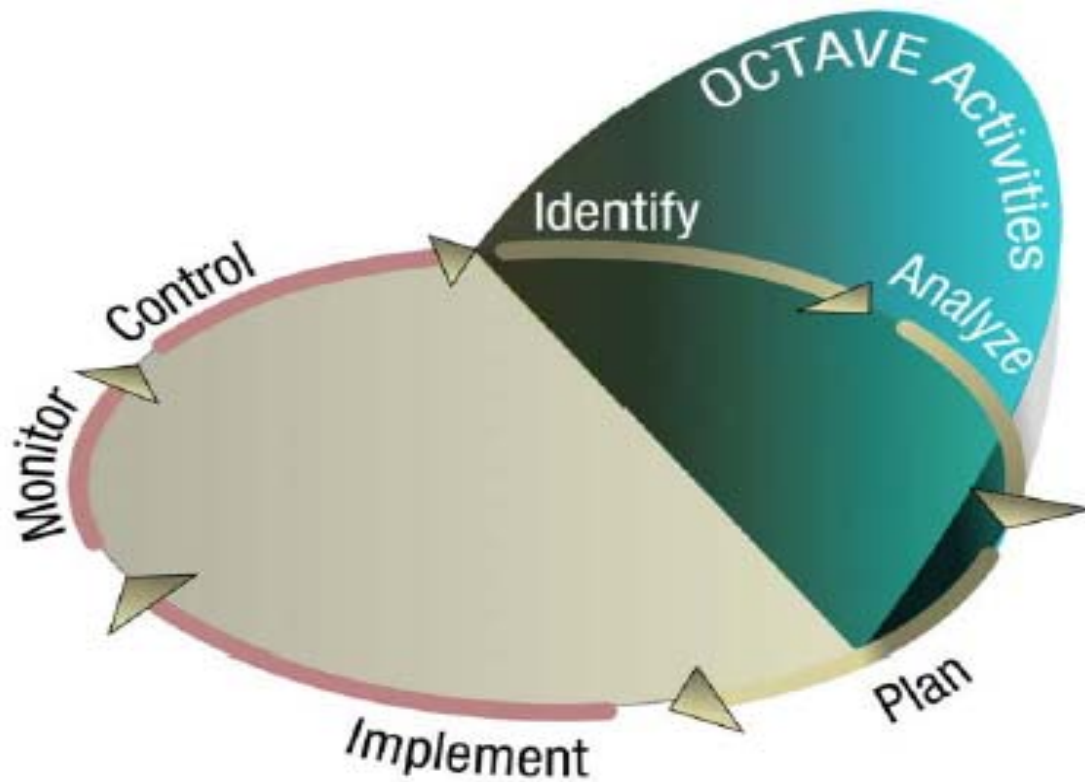
- Case studies
- Lessons learned
- Quick references
- Checklists



DRAFT SP 800-37	Guidelines for the Security Certification and Accreditation (C&A) of Federal Information Technology Systems, October 28, 2002
SP 800-48	Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, November 2002
SP 800-47	Security Guide for Interconnecting Information Technology Systems, September 2002
SP 800-46	Security for Telecommuting and Broadband Communications, September 2002
SP 800-45	Guidelines on Electronic Mail Security, September, 2002
SP 800-44	Guidelines on Securing Public Web Servers, September, 2002
DRAFT SP 800-42	Guideline on Network Security Testing, February 4, 2002




OCTAVE and Risk Management





COBIT: An IT Control Framework

- ◆ Starts from the premise that IT needs to deliver the information that the enterprise needs to achieve its objectives.
- ◆ Promotes process focus and process ownership
- ◆ Divides IT into 34 processes belonging to four domains and provides a high level control objective for each
- ◆ Looks at fiduciary, quality and security needs of enterprises, providing seven information criteria that can be used to generically define what the business requires from IT
- ◆ Is supported by a set of over 300 detailed control objectives

- 
- ◆ Planning
 - ◆ Acquiring & Implementing
 - ◆ Delivery & Support
 - ◆ Monitoring

- 
- ◆ Effectiveness
 - ◆ Efficiency
 - ◆ Availability
 - ◆ Integrity
 - ◆ Confidentiality
 - ◆ Reliability
 - ◆ Compliance



What about ITIL?

- ITIL = Information Technology Infrastructure Library
- Focus is ... IT
- Complete new lexicon
- Geared for IT organizations to talk to each other
Not geared to help ***IT talk to business***



ISO 17799

- Two versions
ISO 17799:2000 and :2005 (27002)
- “Establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization”
- Key message:
“The control objectives and controls in ISO/IEC 17799:2005 are intended to be implemented to meet the requirements identified by a risk assessment.”



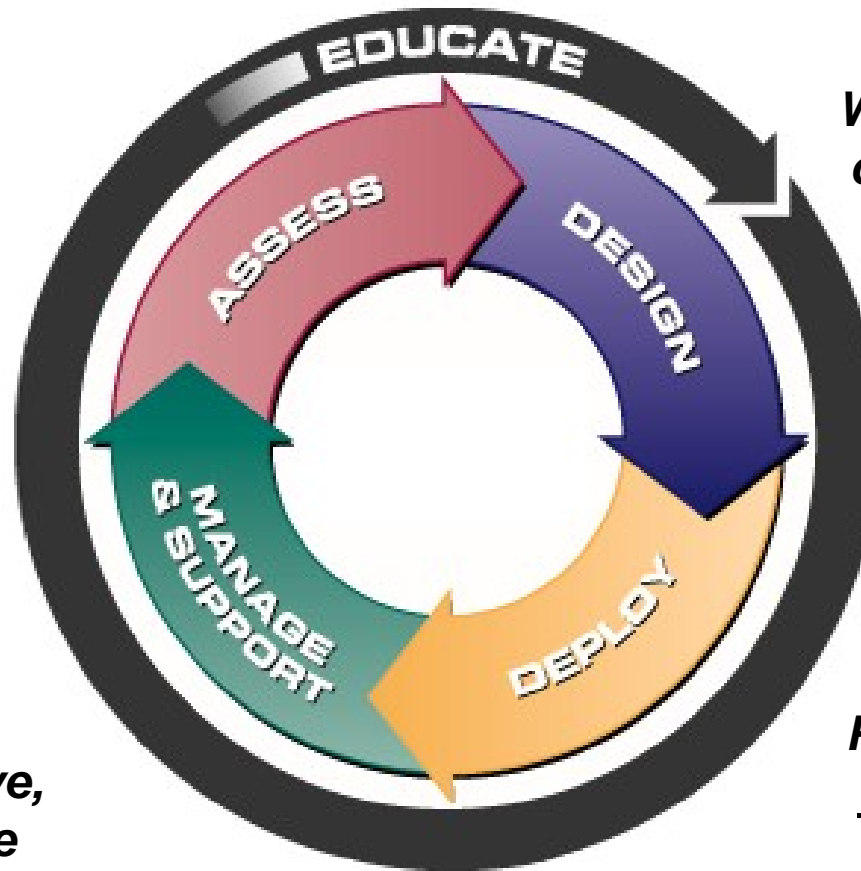
Obtaining good and timely information

- Do you have skills in-house to stay on top of threats and vulnerabilities?
- Does your staff respond to attacks frequently enough to keep their skills sharp?
- Do you have (and follow) escalation, notification and handling procedures?
- What is the value of a second opinion when you think you're under attack?
- Can you conduct a forensic investigation without contaminating evidence?
- What are your regulatory requirements?



Information Security Lifecycle

How well are we protected, now and in the future?



What can we add or change to improve our security?

Given what we have, how do we handle security incidents?

Put all this in place without impacting users



How would you answer these questions?

- Have you evaluated how risks to your business' facilities, personnel, infrastructure, information systems, communications and ongoing operations are evolving?
- Have you determined the impacts of those risks?
- What are your plans to contain (mitigate) these risks?

A business should be able to...

... rapidly adapt and respond to internal or external dynamic changes -- opportunities, demands, disruptions or threats -- and continue operations with limited impact to the business.

This is Understanding IT Governance and Risk Management.





Quick ^ A Scientific Survey





Scientific Survey

My Boss's "Top 3" Hot Buttons Are:

- 1) _____
- 2) _____
- 3) _____

My Boss's Security Awareness: 1 2 3 4 5 (best)

My predecessor left my job because:

If I could talk to my predecessor, the top 3 things I would like to know are:

- 1) _____
- 2) _____
- 3) _____

Do I need to challenge my Boss's "Awareness"?



Business Value Proposition

Financial Loss

Direct Financial Loss

Direct Costs

Loss of Productivity

Indirect Financial Loss

Lost Opportunities

Loss of Funding / Reputation

Other Losses

***Legal Liability / Risk
Trust***

***National Security Issues
National Reputation***



Business Value Proposition

Tip #1: Learn from CNN: Use 'sound bites'

Bad: Computer viruses are bad, as you know. Many companies lose a lot of money because of them.

Better*: Every hour of down time costs us \$x, and the average virus attack requires x.x hours to clean up.

Good: For every virus attack we are unable to process x driver's license requests.

Best: By approving the expenditure of \$x for virus prevention we have saved \$y and z hours of staff time.

Tip #2: Share sound bites that work

* Less bad?



Business Value Proposition

Tip #3: Talk liabilities (FUD)

Bad: If our patient information were to be illegally disclosed we could be in *real* trouble, boss.

Better: Because we are a health care organization we are governed by the Federal HIPAA regulations.

Good: Because we are a health care organization we are governed by the Federal HIPAA regulations, and HIPAA has strict penalties for unauthorized disclosure of patient information, even accidental disclosure.

Best: Our HIPAA training program only costs an average of \$65 per employee while a single HIPAA violation can cost \$100,000's of dollars. *That's ROI!*



Business Value Proposition

Tip #4: Use “case studies”, not just facts

Bad: Without proper security someone could change our information. We need to protect against that.

Good: Think, for a moment, about the impact of something as simple as an unauthorized change to someone's date of employment. That's a change that might go unnoticed, and unchallenged, for years but could affect retirement eligibility, payments and other factors and could be almost impossible to fix later. A change of just five years for a k-12 teacher, as an example, could cost our retirement system an additional \$x in payments.



Business Value Proposition

Tip #5: Be the 'teacher', not just the 'expert'

Bad: A top security objective is non-repudiation, in other words, to assure that transactions can not be repudiated.

Good: One of the big concerns in security today, including one of *our* biggest issues, is non-repudiation. Non-repudiation means that if a transaction is challenged, its origin, accuracy and authenticity can be verified beyond any reasonable doubt. This is not just for electronic security, but our tools are different, and, if properly applied, better. Take for example a written signature, it is possible to claim that the signature is a forgery, but its origin can be established. A digital ...



Business Value Proposition

Tip #6: *Ask for opinions, engage in a dialog**

Bad: We must have accountability for all transactions. It will be invaluable when we prosecute the bad guys.

Best: How important is accountability to our organization? What is our policy regarding prosecution of hackers? Is our policy different for outside hackers and malicious insiders? Have we ever tested these policies and procedures? How much of our budget are we willing to devote to proactively gathering evidence and assuring that we have met all forensic rules?

* dialog means two-sided, monolog means one-sided



Business Value Proposition

Tip #7: Openly discuss scenarios / alternatives

Bad: Availability is our #1 objective.

Best: I am working on our availability policy and I wanted to solicit your thoughts on a few points. Should availability be the #1 objective, or should we keep people out of the system who fail to meet certain criteria? For instance, if a person fails to enter the correct password three times, should they be given access to the system after a phone call to the SOC and having their password reset, or should they require an email and/or phone call from their supervisor? Or something else? Should the policy consider local, remote fixed and remote mobile users differently?



Business Value Proposition

Tip #8: Always have an opinion/solution

Never approach management without a defensible opinion and clear solution in mind. You are not asking for your boss to solve your problems – you are trying to clarify the acceptability of your desired solution and the likelihood that it will be accepted.

You are also determining the amount of preparation and awareness training that will be needed to get your desired solution accepted. You know that it is better not to ask than to be turned down and are trying to determine your chances of success before making a formal request.

BUT, always have an open mind, be ready to change or compromise, as needed, in light of new facts.



Business Value Proposition

Tip #9: Learn from IBM: Always be 'selling'

■ Business Value Proposition
Always look for a chance to sell your solution: don't let an opportunity go by. Deliver one clear message at a time, be successful and put another building block in place. Go for achievable 'interim closes' and build your program step-by-step. Have a long term vision.

Use internal communications, emails, newsletters and company events as vehicles for your selling program. Be relentless, but be subtle.



Business Value Proposition

Tip #10: Involve your entire team.

■ Business Value Proposition
Be sure that your team shares your vision, satisfy naysayers or get rid of them and let your team help sell the vision within the organization. Train them, coach them and set them loose. Teach them the 10 tips and let them be your ambassadors.



Business Value Proposition

Business Value Proposition



Confidentiality / Privacy
Information Integrity
Non-Repudiation
Accountability
Availability



Why effective security is so hard to achieve

Increased risk

Accelerating daily barrage of new threats to critical systems and information

Increased complexity

Applications, technologies and threats have grown increasing complex, dramatically increasing vulnerability

Constant change

Security degrades as networks, business requirements and risks continuously change

Information overload

Daily volume of security information and intelligence can't be effectively analyzed

Limited expertise

Few companies can afford the necessary expertise in-house to adequately address security



Multi-layered Defense